UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

J.W., a minor, by and through her guardian, Angela Johnson, CRYSTAL SCHULTZ, MICHELE EUSEBE, JUSTIN MEDINA, ARTHUR PODROYKIN, and KATHERINE CHAUDHRY, on behalf of themselves and all others similarly situated, Plaintiffs, v. LIVANOVA USA, INC., Defendant.	**CONSOLIDATED ACTION** **CIVIL ACTION NO. 4:24-cv-02250**

CONSOLIDATED CLASS ACTION COMPLAINT

1. Representative Plaintiffs J.W., by and through her guardian, Angela Johnson, Crystal Schultz, Michele Eusebe, Justin Medina, Arthur Podroykin, and Katherine Chaudhry ("Representative Plaintiffs") bring this class action against Defendant LivaNova USA, Inc. ("Defendant") for its failure to properly secure and safeguard Representative Plaintiffs' and Class Members' protected health information and personally identifiable information stored within Defendant's information network, including, without limitation, names, phone numbers, email addresses, postal addresses, dates of birth, medical information (treatment, condition, diagnosis, physician, medical record number and device serial number), and health insurance information (these types of information, *inter alia*, being thereafter referred to, collectively, as "protected

health information" or "PHI"[1] and "personally identifiable information" or "PII").[2] All such information is referred to in the aggregate herein as "PHI/PII."

2. With this action, Representative Plaintiffs seeks to hold Defendant responsible for the harms it caused and will continue to cause Representative Plaintiffs and thousands of other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on November 19, 2023, by which cybercriminals infiltrated Defendant's inadequately protected network and accessed the PHI/PII which was being kept under-protected (the "Data Breach").

3. Representative Plaintiffs further seek to hold Defendant responsible for not ensuring that the PHI/PII was maintained in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) and other relevant standards.

4. While Defendant claims to have discovered the breach as early as November 19, 2023, the Data Breach occurred around October 26, 2023. Defendant did not begin informing victims of the Data Breach until June 17, 2024 and failed to inform victims when or for how long the Data Breach occurred. Indeed, Representative Plaintiffs and Class Members were wholly

[1] Protected health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

unaware of the Data Breach until they received letters from Defendant informing them of it. The Notice received by Representative Plaintiffs was dated June 17, 2024.

5. Defendant acquired, collected and stored Representative Plaintiffs' and Class Members' PHI/PII. Therefore, at all relevant times, Defendant knew or should have known that Representative Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PHI/PII.

6. HIPAA establishes national minimum standards for the protection of individuals' medical records and other protected health information. HIPAA generally applies to health plans and insurers, healthcare clearinghouses and those healthcare providers that conduct certain healthcare transactions electronically and sets minimum standards for Defendant's maintenance of Representative Plaintiffs' and Class Members' PHI/PII. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendant to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiffs' and Class Members' PHI/PII, including rights to examine and obtain copies of their health records and to request corrections thereto.

7. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is created, received, used or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

8. By obtaining, collecting, using and deriving a benefit from Representative Plaintiffs' and Class Members' PHI/PII, Defendant assumed legal and equitable duties to those

individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles. Representative Plaintiffs do not bring claims in this action for direct violations of HIPAA, but charge Defendant with various legal violations merely predicated upon the duties set forth in HIPAA.

9. Defendant disregarded the rights of Representative Plaintiffs and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiffs' and Class Members' PHI/PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Representative Plaintiffs' and Class Members' PHI/PII was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Representative Plaintiffs and Class Members in the future. Representative Plaintiffs and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class and at least one other Class Member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

12. Defendant is headquartered and routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiffs' claims took place within this District, and Defendant does business in this Judicial District.

PLAINTIFFS

Plaintiff J.W. by and through her Guardian, Angela Johnson

14. Plaintiff J.W. is a minor child who brings this suit through her grandmother and guardian, Angela Johnson. At all relevant times herein, Plaintiff J.W. was a resident and citizen of the state of Illinois. Plaintiff J.W. is a victim of the Data Breach.

15. Defendant received highly sensitive PHI/PII from Plaintiff J.W. in connection with the services Plaintiff obtained. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

16. At all times herein relevant, Plaintiff J.W. is a member of the Class.

17. Plaintiff J.W.'s PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's PHI/PII. Plaintiff J.W.'s PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

18. Plaintiff J.W. received a letter from Defendant stating Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

19. As a result, Plaintiff J.W. spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact

of the Data Breach, exploring credit monitoring and identity theft insurance options and self-monitoring Plaintiff's accounts and credit reports. This time has been lost forever and cannot be recaptured.

20. Plaintiff J.W. suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

21. Plaintiff J.W. suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

22. Plaintiff J.W. suffered imminent and impending injury arising from the substantially increased lifetime risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII being placed in the hands of unauthorized third parties/criminals.

23. Plaintiff J.W. has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Michele Eusebe

24. Plaintiff Michele Eusebe is an adult individual and, at all relevant times herein, was a resident and citizen of the state of Georgia. Plaintiff Eusebe is a victim of the Data Breach.

25. Defendant received highly sensitive PHI/PII from Plaintiff Eusebe in connection with the services Plaintiff obtained. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

26. At all times herein relevant, Plaintiff Eusebe is a member of the Class.

27. Plaintiff Eusebe's PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

28. Plaintiff Eusebe received a letter from Defendant stating Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

29. As a result, Plaintiff Eusebe spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and credit reports. This time has been lost forever and cannot be recaptured.

30. Plaintiff Eusebe suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

31. Plaintiff Eusebe suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

32. Plaintiff Eusebe suffered imminent and impending injury arising from the substantially increased lifetime risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII being placed in the hands of unauthorized third parties/criminals.

33. Plaintiff Eusebe has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Crystal Shultz

34. Plaintiff Crystal Shultz is an adult individual and, at all relevant times herein, was a resident and citizen of the state of New York. Plaintiff Schultz is a victim of the Data Breach.

35. Defendant received highly sensitive PHI/PII from Plaintiff Schultz in connection with the services Plaintiff obtained. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

36. At all times herein relevant, Plaintiff Schultz is a member of the Class.

37. Plaintiff Schultz's PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

38. Plaintiff Schultz received a letter from Defendant stating Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

39. As a result, Plaintiff Schultz spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and credit reports. This time has been lost forever and cannot be recaptured.

40. Plaintiff Schultz suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

41. Plaintiff Schultz suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

42. Plaintiff Schultz suffered imminent and impending injury arising from the substantially increased liftetime risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII being placed in the hands of unauthorized third parties/criminals.

43. Plaintiff Schultz has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Justin Medina

44. Plaintiff Justin Medina is an adult individual and, at all relevant times herein, was a resident and citizen of the state of Washington. Plaintiff Medina is a victim of the Data Breach.

45. Defendant received highly sensitive PHI/PII from Plaintiff Medina in connection with the services Plaintiff obtained. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

46. At all times herein relevant, Plaintiff Medina is a member of the Class.

47. Plaintiff Medina's PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

48. Plaintiff Medina received a letter from Defendant stating Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

49. As a result, Plaintiff Medina spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and credit reports. This time has been lost forever and cannot be recaptured.

50. Plaintiff Medina suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

51. Plaintiff Medina suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

52. Plaintiff Medina suffered imminent and impending injury arising from the substantially increased lifetime risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII being placed in the hands of unauthorized third parties/criminals.

53. Plaintiff Medina has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Arthur Podroykin

54. Plaintiff Arthur Podroykin is an adult individual and, at all relevant times herein, was a resident and citizen of the state of Illinois. Plaintiff Podroykin is a victim of the Data Breach.

55. Defendant received highly sensitive PHI/PII from Plaintiff Podroykin in connection with the services Plaintiff obtained. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

56. At all times herein relevant, Plaintiff Podroykin is a member of the Class.

57. Plaintiff Podroykin's PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

58. Plaintiff Podroykin received a letter from Defendant stating Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

59. As a result, Plaintiff Podroykin spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and credit reports. This time has been lost forever and cannot be recaptured.

60. Plaintiff Podroykin suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

61. Plaintiff Podroykin suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff's PHI/PII.

62. Plaintiff Podroykin suffered imminent and impending injury arising from the substantially increased liftetime risk of fraud, identity theft and misuse resulting from Plaintiff's PHI/PII being placed in the hands of unauthorized third parties/criminals.

63. Plaintiff Podroykin has a continuing interest in ensuring that Plaintiff's PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Katherine Chaudry

64. Plaintiff Katherine Chaudhry is an adult individual and, at all relevant times herein, was a resident and citizen of the state of New York. Plaintiff Chaudhry is a victim of the Data Breach.

65. Defendant received highly sensitive PHI/PII from Plaintiff Chaudhry in connection with the services Plaintiff obtained. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

66. At all times herein relevant, Plaintiff Chaudhry is and was a member of the Class.

67. Plaintiff Chaudhry's PHI/PII was exposed in the Data Breach because Defendant stored and/or shared Plaintiff's PHI/PII. Plaintiff's PHI/PII was within the possession and control of Defendant at the time of the Data Breach.

68. Plaintiff Chaudhry received a letter from Defendant stating Plaintiff's PHI/PII was involved in the Data Breach (the "Notice").

69. As a result, Plaintiff Chaudhry spent time dealing with the consequences of the Data Breach, which included, and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring Plaintiff's accounts and credit reports. This time has been lost forever and cannot be recaptured.

70. Plaintiff Chaudhry suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PHI/PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

71. Plaintiff Chaudhry suffered lost time, annoyance, interference and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling Plaintiff Chaudhry's PHI/PII.

72. Plaintiff Chaudhry suffered imminent and impending injury arising from the substantially increased lifetime risk of fraud, identity theft and misuse resulting from Plaintiff Chaudhry's PHI/PII being placed in the hands of unauthorized third parties/criminals.

73. Plaintiff Chaudhry has a continuing interest in ensuring that Plaintiff Chaudhry's PHI/PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

74. Defendant LivaNova USA, Inc. is a corporation organized under the state laws of Delaware with its principal place of business located at 100 Cyberonics Blvd., Houston, Texas 77058. The registered agent for service of process is Universal Registered Agents, Inc., 7533 County Road 1127, Godley, TX 76044. Defendant is a global medical technology company distributing products and therapies worldwide[3].

75. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiffs. Representative Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

76. Representative Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiffs and the following class (the "Class"):

[3] https://www.livanova.com/en-us/about-us (accessed September 14, 2024).

Nationwide Class

All persons in the United States of America whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on or before October 26, 2023.

77. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including, but not limited to, its departments, agencies, divisions, bureaus, boards, sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

78. Moreover, pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as appropriate, and (c)(4), Representative Plaintiffs seek certification of state common law claims in the alternative to the nationwide claims, as well as statutory claims under state consumer protection on behalf of subclasses for residents of Illinois, New York (collectively, "State Subclasses").

Georgia Subclass

All residents of Georgia whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on or before October 26, 2023.

Illinois Subclass

All residents of Illinois whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on or before October 26, 2023.

New York Subclass

All residents of New York whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on or before October 26, 2023.

Washington Subclass

All residents of Washington whose PHI/PII was exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on or before October 26, 2023.

79. Representative Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and its motion for class certification.

80. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Class are so numerous that joinder of all members is impractical, if not impossible. Membership in the Class will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiffs and Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Representative Plaintiffs and the Class to exercise due care in collecting, storing, using and/or safeguarding their PHI/PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiffs and Class Members that their PHI/PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiffs' and Class Members' PHI/PII;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiffs' and Class Members' PHI/PII;

11) Whether Representative Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct; and

12) Whether Representative Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Representative Plaintiffs' claims are typical of the claims of the Plaintiff Class. Representative Plaintiffs and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiffs in this class action are adequate representatives of the Plaintiff Class in that Representative Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members

or the Class in its entirety. Representative Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests.

81. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

82. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Representative Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Representative Plaintiffs.

83. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI/PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

84. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the

Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

85. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' PHI/PII. Representative Plaintiffs were among the individuals whose data was accessed in the Data Breach.

86. According to the Data Breach Notification and/or publicly filed documents, Representative Plaintiffs state, based on information and belief, that thousands of persons were affected by the Data Breach.

Representative Plaintiffs were provided the information detailed above upon Representative Plaintiffs' receipt of a letter from Defendant. Representative Plaintiffs were not aware of the Data Breach until receiving that letter.

Defendant's Failed Response to the Data Breach

87. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiffs' and Class Members' PHI/PII with the intent of misusing the PHI/PII, including marketing and selling Representative Plaintiffs' and Class Members' PHI/PII.

88. Not until long after it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PHI/PII Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

89. Defendant had and continues to have obligations created by HIPAA, applicable federal and state law as set forth herein, reasonable industry standards, common law and its own

assurances and representations to keep Representative Plaintiffs' and Class Members' PHI/PII confidential and to protect such PHI/PII from unauthorized access.

90. Representative Plaintiffs and Class Members were required to provide their PHI/PII to Defendant in order to receive services. Thus, Defendant created, collected and stored Representative Plaintiffs' and Class Members' PHI/PII with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

91. Despite this, Representative Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used and what steps are being taken, if any, to secure their PHI/PII going forward. Representative Plaintiffs and Class Members are thus left to speculate as to where their PHI/PII ended up, who has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

92. Representative Plaintiffs' and Class Members' PHI/PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PHI/PII for targeted marketing without Representative Plaintiffs' and/or Class Members' approval. Either way, unauthorized individuals can now easily access Representative Plaintiffs' and Class Members' PHI/PII.

Defendant Collected/Stored Class Members' PHI/PII

93. Defendant acquired, collected, stored and assured reasonable security over Representative Plaintiffs' and Class Members' PHI/PII.

94. As a condition of its relationships with Representative Plaintiffs and Class Members, Defendant required that Representative Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PHI/PII. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Data Breach.

95. By obtaining, collecting and storing Representative Plaintiffs' and Class Members' PHI/PII, Defendant assumed legal and equitable duties over the PHI/PII and knew or should have known that it was thereafter responsible for protecting Representative Plaintiffs' and Class Members' PHI/PII from unauthorized disclosure.

96. Representative Plaintiffs and Class Members have taken reasonable steps to maintain their PHI/PII's confidentiality. Representative Plaintiffs and Class Members relied on Defendant to keep their PHI/PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

97. Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Representative Plaintiffs' and Class Members' PHI/PII.

98. Defendant's negligence in safeguarding Representative Plaintiffs' and Class Members' PHI/PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

99. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with the resources to put adequate data security protocols in place.

100. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Representative Plaintiffs' and Class Members' PHI/PII from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

101. In failing to adequately secure Representative Plaintiffs' and Class Member's sensitive data, Defendant breached duties it owed Representative Plaintiffs and Class Members under statutory and common law.

102. Representative Plaintiffs and Class Members surrendered their highly sensitive PHI/PII to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their PHI/PII, independent of any statute.

103. Moreover, under HIPAA, health insurance providers have an affirmative duty to keep patients' PHI/PII confidential. As a covered entity, Defendant has a statutory duty under HIPAA and other federal and state statutes to safeguard Representative Plaintiffs' and Class Members' PHI/PII.

104. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information") and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

105. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

106. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

107. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is "individually identifiable health information […] that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

108. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

109. HIPAA also requires Defendant to "review and modify the security measures implemented […] as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1). Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

110. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

111. In addition to its obligations under federal and state laws, Defendant owed a duty to Representative Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Representative Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks and protocols adequately protected Representative Plaintiffs' and Class Members' PHI/PII.

112. Defendant owed a duty to Representative Plaintiffs and Class Members to design, maintain and test its computer systems, servers and networks to ensure that all PHI/PII in its possession was adequately secured and protected.

113. Defendant owed a duty to Representative Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect all PHI/PII in its possession, including not sharing information with other entities who maintained substandard data security systems.

114. Defendant owed a duty to Representative Plaintiffs and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

115. Defendant owed a duty to Representative Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

116. Defendant owed a duty to Representative Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft because such an inadequacy would be a material fact in the decision to entrust their PHI/PII to Defendant.

117. Defendant owed a duty of care to Representative Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

118. Defendant owed a duty to Representative Plaintiffs and Class Members to encrypt and/or more reliably encrypt Representative Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

119. While the greater efficiency of electronic health records translates to cost savings for providers, it also comes with the risk of privacy breaches. These electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, medical prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers and other personal information on a number of underground internet websites.

120. The high value of PHI/PII to criminals is further evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[4] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[5] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[6]

121. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[7] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[8] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[9]

122. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiffs and Class Members. For example, it is believed that certain PHI/PII compromised in the 2017 Equifax data breach was being used three years later by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

---

4 *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

5 *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

6 *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

7 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/.

8 https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.

9 https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/.

123. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

124. Identity thieves can use PHI/PII, such as that of Representative Plaintiffs and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

125. The ramifications of Defendant's failure to keep secure Representative Plaintiffs' and Class Members' PHI/PII are long lasting and severe. Once PHI/PII is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Representative Plaintiffs' and Class Members' PHI/PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PHI/PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

126. There may be a time lag between when harm occurs versus when it is discovered and also between when PHI/PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen

> data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

127. The harm to Representative Plaintiffs and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[11]

128. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[12]

129. When cybercriminals access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Representative Plaintiffs and Class Members.

130. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while

---

[10] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf/.
[11] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.
[12] *Id*.
[13] Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[14]

131. And data breaches are preventable.[15] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[16] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…."[17]

132. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[18]

133. Here, Defendant knew of the importance of safeguarding PHI/PII and of the foreseeable consequences that would occur if Representative Plaintiffs' and Class Members' PHI/PII was stolen, including the significant costs that would be placed on Representative Plaintiffs and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Representative Plaintiffs and Class Members. Its failure to do so is therefore intentional, willful, reckless and/or grossly negligent.

---

[14] *Id.*; *see also* Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[15] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[16] *Id.* at 17.

[17] *Id.* at 28.

[18] *Id.*

134. Defendant disregarded the rights of Representative Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions, (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiffs' and Class Members' PHI/PII, (iii) failing to take standard and reasonably available steps to prevent the Data Breach, (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time, and (v) failing to provide Representative Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of Representative Plaintiffs and the Nationwide Class)

135. Each and every allegation of the preceding paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

136. At all times herein relevant, Defendant owed Representative Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PHI/PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing Representative Plaintiffs' and Class Members' PHI/PII on its computer systems.

137. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PHI/PII in its possession;

b. to protect Representative Plaintiffs' and Class Members' PHI/PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their PHI/PII.

138. Defendant knew that the PHI/PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Representative Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

139. Defendant knew or should have known of the risks inherent in collecting and storing PHI/PII, the vulnerabilities of its data security systems and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

140. Defendant knew or should have known that its data systems and networks did not adequately safeguard Representative Plaintiffs' and Class Members' PHI/PII.

141. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PHI/PII that Representative Plaintiffs and Class Members had entrusted to it.

142. Defendant breached its duties to Representative Plaintiffs and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' PHI/PII.

143. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Representative Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PHI/PII contained thereon.

144. Representative Plaintiffs' and Class Members' willingness to entrust Defendant with its PHI/PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PHI/PII stored

on them from attack. Thus, Defendant had a special relationship with Representative Plaintiffs and Class Members.

145. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Representative Plaintiffs' and Class Members' PHI/PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Representative Plaintiffs and/or the remaining Class Members.

146. Defendant breached its general duty of care to Representative Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Representative Plaintiffs' and Class Members' PHI/PII;

b. by failing to timely and accurately disclose that Representative Plaintiffs' and Class Members' PHI/PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PHI/PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PHI/PII;

d. by failing to provide adequate supervision and oversight of the PHI/PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Representative Plaintiffs' and Class Members' PHI/PII, misuse the PHI/PII and intentionally disclose it to others without consent;

e. by failing to adequately train its employees to not store PHI/PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiffs' and the Class Members' PHI/PII;

g. by failing to implement processes to quickly detect data breaches, security incidents or intrusions; and

h. by failing to encrypt Representative Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

147. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

148. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Representative Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

149. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PHI/PII to Representative Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PHI/PII.

150. Defendant breached its duty to notify Representative Plaintiffs and Class Members of the unauthorized access by waiting excessively after learning of the Data Breach to notify Representative Plaintiffs and Class Members and then by failing and continuing to fail to provide Representative Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Representative Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Representative Plaintiffs and Class Members.

151. Further, through its failure to provide timely and clear notification of the Data Breach to Representative Plaintiffs and Class Members, Defendant prevented Representative Plaintiffs and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or access their PHI/PII.

152. There is a close causal connection between Defendant's failure to implement security measures to protect Representative Plaintiffs' and Class Members' PHI/PII and the harm suffered, or risk of imminent harm suffered, by Representative Plaintiffs and Class Members.

Representative Plaintiffs' and Class Members' PHI/PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI/PII by adopting, implementing and maintaining appropriate security measures.

153. Defendant's wrongful actions, inactions and omissions constituted (and continue to constitute) common law negligence.

154. The damages Representative Plaintiffs and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

155. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI/PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

156. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect PHI/PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiffs and Class Members.

157. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer injury, including, but not limited to, (i) actual identity theft, (ii) the loss of the opportunity of how their PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft, tax fraud and/or unauthorized use

of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the continued risk to their PHI/PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Representative Plaintiffs' and Class Members' PHI/PII in its continued possession, and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Representative Plaintiffs and Class Members.

158. As a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy and other economic and noneconomic losses.

159. Additionally, as a direct and proximate result of Defendant's negligence, Representative Plaintiffs and Class Members have suffered and will continue to suffer the continued risks of exposure of their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PHI/PII in its continued possession.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract and Breach of Implied Covenant of Good Faith and Fair Dealing
(On behalf of Representative Plaintiffs and the Nationwide Class)

160. Paragraphs 1 through 134 above are incorporated in this Count with the same force and effect as though fully set forth herein.

161. Through their course of conduct, Defendant, Representative Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Representative Plaintiffs' and Class Members' PHI/PII.

162. Defendant solicited, invited and required Representative Plaintiffs and Class Members to provide their PHI/PII as part of Defendant's regular business practices. Representative Plaintiffs and Class Members accepted Defendant's offers by, in part, providing their PHI/PII to Defendant.

163. As a condition of being direct customers and/or employees of Defendant, Representative Plaintiffs and Class Members provided and entrusted their PHI/PII to Defendant. In so doing, Representative Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Representative Plaintiffs and Class Members if its data had been breached and compromised or stolen.

164. A meeting of the minds occurred when Representative Plaintiffs and Class Members agreed to, and did, provide their PHI/PII to Defendant, in exchange for, amongst other things, the protection of their PHI/PII.

165. Representative Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

166. Defendant breached the implied contracts it made with Representative Plaintiffs and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

167. Moreover, Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PHI/PII, failing to timely and accurately disclose the Data Breach to Representative Plaintiffs and Class Members and continued acceptance of PHI/PII and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

168. Defendant acted in bad faith and/or with malicious motive in denying Representative Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

169. As a direct and proximate result of Defendant's above-described breach of implied contract, Representative Plaintiffs and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (f) other economic and noneconomic harm.

THIRD CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of Representative Plaintiffs and the Nationwide Class)

170. Paragraphs 1 through 134 above are incorporated in this Count with the same force and effect as though fully set forth therein.

171. Representative Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid the Defendant and/or its agents for medical products and/or

services that were the subject of the transaction and, in doing so, provided Defendant with their PHI/PII.

172. Defendant knew that Representative Plaintiffs and Class Members conferred a monetary benefit upon it and has accepted and retained that benefit by accepting and retaining the PHI/PII entrusted to it. Defendant profited from Representative Plaintiffs' retained data and used Plaintiffs' and Class Members' PHI/PII for business purposes.

173. Defendant failed to secure Representative Plaintiffs' and Class Members' PHI/PII and, therefore, did not fully compensate Representative Plaintiffs and Class Members for the value that their PHI/PII provided.

174. Defendant acquired the PHI/PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

175. If Representative Plaintiffs and Class Members had known that Defendant would not use adequate data security practices to monitor, supervise, and secure their PHI/PII, they would not have entrusted Defendant with their PHI/PII or obtained medical products and/or services from Defendant.

176. Representative Plaintiffs and Class Members have no adequate remedy at law.

177. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Representative Plaintiffs' and Class Members' PHI/PII. Under these circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

178. As a direct and proximate result of Defendant's conduct, Representative Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy, (ii) theft of their PHI/PII, (iii) lost or diminished value of PHI/PII, (iv) lost time and

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, (v) loss of benefit of the bargain, (vi) statutory damages, (vii) nominal damages, and (viii) the continued and certainly increased risk that their PHI/PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse, and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PHI/PII.

FOURTH CLAIM FOR RELIEF
Violation of Illinois Consumer Fraud Act
815 Ill. Comp. Stat. §§ 505, *et seq.*
(On behalf of Illinois Plaintiffs J.W. and Podroykin and the Illinois Subclass)

179. Paragraphs 1 through 134 above are incorporated in this Count with the same force and effect as though fully set forth therein.

180. The Illinois Plaintiffs J.W. and Arthur Podroykin individually (hereinafter "Plaintiffs" for purposes of this Count only) and on behalf of the Illinois Subclass, bring this claim.

181. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

182. Plaintiffs and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

183. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

184. Defendant's deceptive, unfair and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Illinois Subclass Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks and adequately maintain and/or improve security and privacy measures, which was a direct and proximate

cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, Illinois laws regulating the use and disclosure of Social Security numbers, 815 Ill. Comp. Stat § 505/2RR and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Illinois Subclass Members' PII/PHI, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Illinois Subclass Members' PII/PHI; and

g. Omitting, suppressing and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, Illinois laws regulating the use and disclosure of Social Security numbers, 815 Ill. Comp. Stat § 505/2RR and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

185. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII/PHI.

186. Defendant intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

187. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid, and this substantial injury outweighed any benefits to consumers or to competition.

188. Defendant acted intentionally, knowingly and maliciously to violate Illinois's Consumer Fraud Act and recklessly disregarded Plaintiffs' and Illinois Subclass Members' rights.

189. As a direct and proximate result of Defendant's unfair, unlawful and deceptive acts and practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PII/PHI.

190. Plaintiffs and Illinois Subclass Members seek all monetary and nonmonetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief and reasonable attorneys' fees and costs.

FIFTH CLAIM FOR RELIEF
Violation of N.Y. Gen. Bus. Law §§ 349 *et seq.*
(On behalf of New York Plaintiffs Shultz and Chaudhry and the New York Subclass)

191. Paragraphs 1 through 134 above are incorporated in this Count with the same force and effect as though fully set forth therein.

192. The New York Plaintiffs Kristen Shultz and Katherine Chaudhry individually (hereinafter "Plaintiffs" for purposes of this Count only) and on behalf of the New York Subclass, bring this claim.

193. Defendant engaged in deceptive acts or practices in the conduct of its business,

trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PHI/PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PHI/PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass Members' PHI/PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

194. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PHI/PII.

195. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass Members'

rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

196. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PHI/PII; overpayment for Defendant's services; loss of the value of access to their PHI/PII; and the value of identity protection services made necessary by the Data Breach.

197. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the New Yorkers affected by the Data Breach.

198. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

199. As a direct and proximate result of Defendant's unfair, unlawful and deceptive acts and practices, Plaintiffs and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PII/PHI.

200. Plaintiffs and New York Subclass Members seek all monetary and nonmonetary

relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, punitive damages, injunctive relief and reasonable attorneys' fees and costs.

SIXTH CLAIM FOR RELIEF
Violation of Washington Consumer Protection Act
Wash. Rev. Code §§ 19.86.020 *et seq.*
(On behalf of Washington Plaintiff Medina and the Washington Subclass)

201. Paragraphs 1 through 134 above are incorporated in this Count with the same force and effect as though fully set forth therein.

202. The Washington Plaintiff Justin Medina individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the Washington Subclass, brings this claim

203. Defendant is a "person," as defined by Wash. Rev. Code § 19.86.010(1).

204. Defendant advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code § 19.86.010 (2).

205. Defendant engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass members' PHI/PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of

Plaintiffs' and Subclass members' PHI/PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass Members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Subclass members' PHI/PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PHI/PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

206. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PHI/PII.

207. Defendant acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass Members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

208. Defendant's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons.

209. Further, its conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

210. As a direct and proximate result of Defendant's unfair, unlawful and deceptive acts and practices, Plaintiffs and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and nonmonetary damages,

including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their PII/PHI.

211. Plaintiff and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

SEVENTH CLAIM FOR RELIEF
Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*
(On behalf of Representative Plaintiffs and the Nationwide Class)

212. Paragraphs 1 through 134 above are incorporated in this Count with the same force and effect as though fully set forth therein.

213. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

214. An actual controversy has arisen in the wake of the Data Breach regarding Representative Plaintiffs' and Class Members' PHI/PII and whether Defendants are currently maintaining data security measures adequate to protect Representative Plaintiffs and Class Members from further data breaches that compromise their PHI/PII. Representative Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Representative Plaintiffs continue to suffer injuries as result of the compromise of their PHI/PII and remains at imminent risk that further compromises of their PII will occur in the future.

215. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (a) Defendant owes a legal duty to

secure PII and to timely notify impacted individuals of a data breach under the common law, Section 5 of the FTC Act, and various state statutes, and (b) Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII in its possession.

216. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect PII in Defendant's possession and control.

217. If an injunction is not issued, Representative Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Representative Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

218. The hardship to Representative Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Representative Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

219. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Representative Plaintiffs and Class Members whose confidential information would be further compromised

RELIEF SOUGHT

WHEREFORE, Representative Plaintiffs, on their own behalf and on behalf of each member of the proposed Nationwide Class and State Subclasses\, respectfully request that the Court enter judgment in favor of Representative Plaintiffs and the Class and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify the proposed Class under Federal Rules of Civil Procedure Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including actual, nominal and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiffs' and Class Members' PHI/PII, and from refusing to issue prompt, complete and accurate disclosures to Representative Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiffs and Class Members, including, but not limited to, an Order:

   a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards and federal, state or local laws;

c. requiring Defendant to delete and purge Representative Plaintiffs' and Class Members' PHI/PII unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiffs and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiffs' and Class Members' PHI/PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

f. prohibiting Defendant from maintaining Representative Plaintiffs' and Class Members' PHI/PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PHI/PII, as well as protecting the PHI/PII of Representative Plaintiffs and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs and litigation expenses, as allowed by law; and

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiffs, individually, and on behalf of the Plaintiff Class, hereby demand a trial by jury for all issues triable by jury.

Dated: September 23, 2024

By: /s/ Scott Edward Cole

Scott Edward Cole, Esq. (CA S.B. #160744)*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com

Joe Kendall, Esq.
TX S.B. #11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: (214) 744-3000
Facsimile: (214) 744-3015
Email: jkendall@kendalllawgroup.com

Mariya Weekes, Esq.*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, Florida 33134
Telephone: (786) 879-8200
Facsimile: (786) 879-7520
Email: mweekes@milberg.com

Jeff Ostrow, Esq.*
KOPELOWITZ OSTROW FERGUSON WISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 332-4200
Email: ostrow@kolawyers.com

Ronald W. Armstrong, Esq.
THE ARMSTRONG FIRM, PLLC
109 Yoalana St, Suite 210
Boerne, Texas 78006
Telephone: (210) 277-0542
Facsimile: (210) 277-0548
Email: rwaii@tafpllc.com

Jarrett L. Ellzey, Esq.
TX S.B. 24040864
Leigh Montgomery, Esq.
TX S.B. #24052214
ELLZEY & ASSOCIATES, PLLC
1105 Milford Street
Houston, Texas 77066
Telephone: (713) 554-2377
Facsimile: (888) 276-3455
Email: jarett@ellzeyaw.com
Email: leigh@ellseylaw.com

Tyler J. Bean, Esq.*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
Email: tbean@sirillp.com

Kevin Laukaitis, Esq.*
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Telephone: (215) 789-4462
Email: klaukaitis@laukaitislaw.com

Attorneys for Representative Plaintiffs
and the Plaintiff Class

**Admitted Pro Hac Vice*

CERTIFICATE OF SERVICE

I hereby certify that, on September 23, 2024, I caused to be filed the foregoing document electronically using the Court's electronic case filing (ECF) system, which will automatically send a notice of electronic filing to the email addresses of all counsel of record.

/s/ Scott Edward Cole